


# Overcoming Technical Challenges in the Windows Baselines

[kurt.dillard.c@g2-inc.com](mailto:kurt.dillard.c@g2-inc.com)

[kurtdillard@msn.com](mailto:kurtdillard@msn.com)

# Agenda

- ▶ What Changed Since Alpha
  - ▶ What Hasn't Changed
  - ▶ How do the USGCB and FDCC Relate?
  - ▶ Building Your Test Lab
  - ▶ Resources
- 

# What Changed

- ▶ **Core Networking – Dynamic Host Configuration Protocol (DHCP–In)**
- ▶ **Core Networking – Dynamic Host Configuration Protocol (DHCPV6–In)**
  - Were: Not configured
  - Now: Enabled: Yes
- ▶ **Debug programs user right**
  - Was: No one
  - Now: Administrators
  - Take control of any process
  - Debug any process including the kernel
  - *Do not give to non-admins*

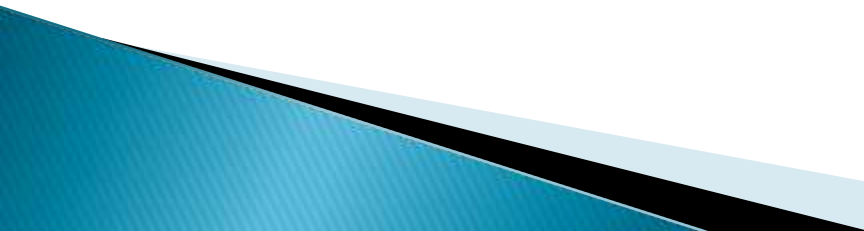
# What Changed Continued...

- ▶ **Do not process the legacy Run list**
  - Was: Enabled
  - Now: Not defined
  - Blocks execution of applications at
    - HKLM\Software\Microsoft\Windows\CurrentVersion\Run
  - Minor speed-bump for malware
    - Requires admin rights to modify the key
    - Dozens of other ways to launch malware at startup if you have admin rights
  - Impact: Numerous legitimate apps

# What Changed Continued...

- ▶ **Require trusted path for credential entry**
  - Was: Enabled
  - Now: Not configured
- ▶ **User Account Control: Behavior of the elevation prompt for standard users**
  - Was: Prompt for credentials
  - Now: Prompt for credentials on the secure desktop
- ▶ **MSS: (NtfsDisable8dot3NameCreation) Enable the computer to stop generating 8.3 style filenames**
  - Was: Enabled
  - Now: Not configured


# What Changed Continued...

- ▶ **Turn off Windows Update device driver search prompt**
  - ▶ **Turn off Windows Update device driver searching**
    - Were: Enabled
    - Now: Not configured
  - ▶ **Turn off Automatic Root Certificates Update**
    - Was: Enabled
    - Now: Not configured
  - ▶ **WLAN AutoConfig system service**
    - Was: Disabled
    - Now: Not configured
- 

# Power Management

- ▶ Systems will hibernate after 20 minutes of inactivity
- ▶ Potentially impacted:
  - Enterprise management
  - Remote Desktop Services (RDS) users
  - Systems that process long running jobs
- ▶ Investigate
  - Wake-on-LAN (WOL)
  - Subnet Directed Broadcasts (SDB)

# Some Settings are Conditional


- ▶ Still mandatory, however...
  - ▶ Under specific conditions agencies may adjust those settings.
  - ▶ Our SCAP 1.0 content does not support conditional logic, so track these as deviations,
  - ▶ SCAP 1.1 content will support conditional logic.
- 




# Conditional Continued...

- ▶ **Access this computer from the network**
- ▶ User right necessary for establishing IPsec connections
  - Limited to Administrators
  - Internet Key Exchange (IKE) fails
  - Granting the right to “Domain Computers” or “Authenticated Users” should resolve it
- ▶ **IPv6 transitional technologies**
  - 6to4, IP-HTTPS, ISATAP, & Teredo


# Conditional Continued...

- ▶ Windows Error Reporting
  - ▶ Remote Assistance
  - ▶ Windows NTP Client
  - ▶ Remote Desktop Services
  - ▶ Windows Updates
  - ▶ Bluetooth
- 

# Agenda

- ▶ What Changed Since Alpha
  - ▶ What Hasn't Changed
  - ▶ How do the USGCB and FDCC Relate?
  - ▶ Building Your Test Lab
  - ▶ Resources
- 

# What Has Not Changed

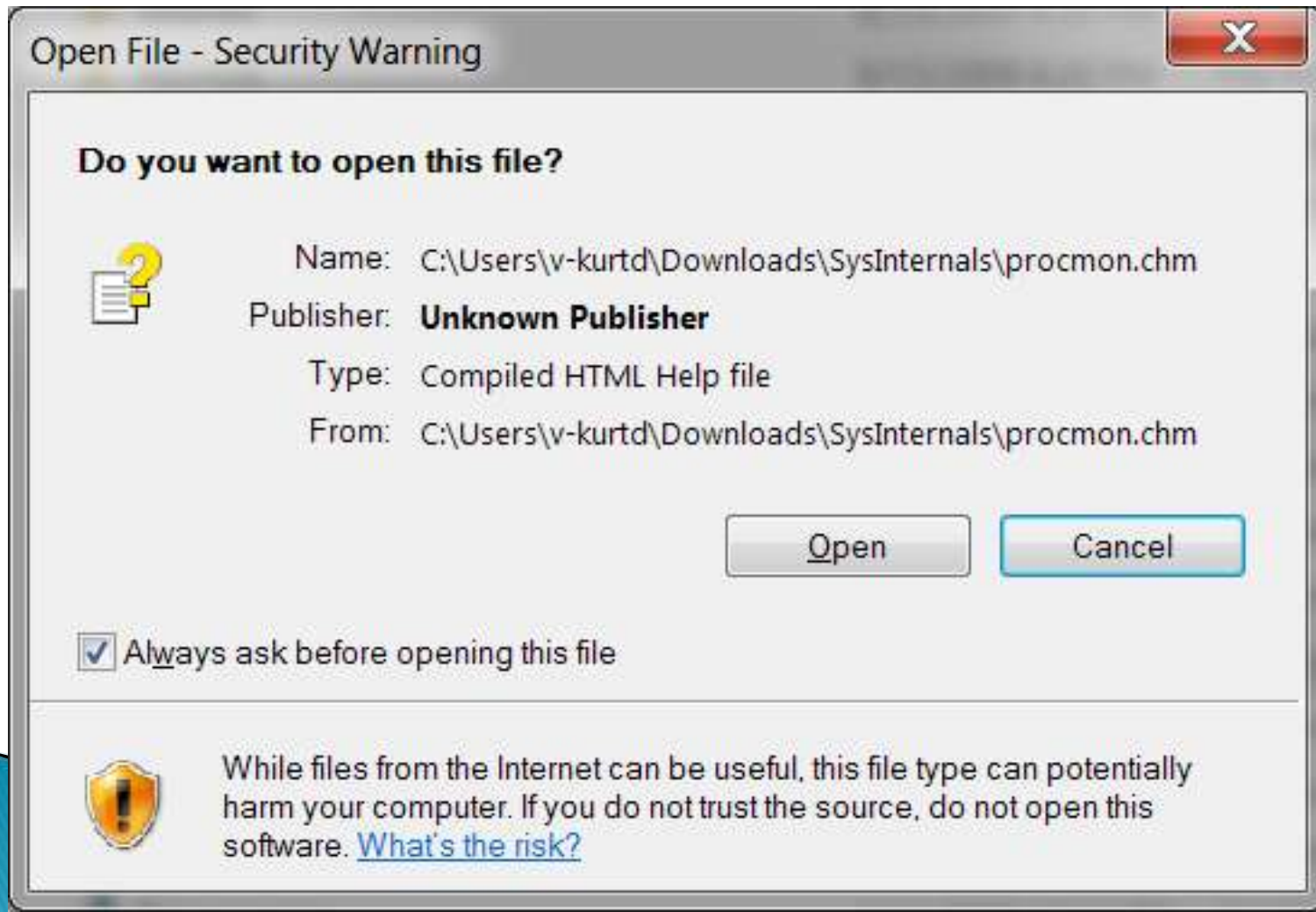
- ▶ Users still cannot have admin privileges
  - ▶ Can't download and install ActiveX controls, add-ons, or Desktop Gadgets
    - Download signed ActiveX controls
    - Download unsigned ActiveX controls
    - Initialize and script ActiveX controls not marked as safe
  - ▶ No prompts
  - ▶ Solutions?
- 

# What Has Not Changed Continued...

- ▶ Windows XP, Windows Server 2003
  - 300+ root certs
  - Impacts performance of many tasks
- ▶ Windows Root Certificate Program
  - Default trusted CAs baked into Windows
  - Vista and later have a couple dozen certs
  - Certs can be added and removed dynamically
- ▶ **Turn off Automatic Root Certificates Update**
  - Disables this feature
  - Lots of files/programs will be treated as “unsigned”
  - Lots of HTTPS web sites will show “invalid cert”

# What Has Not Changed Continued...

- ▶ You know this dialog box?



# What Has Not Changed Continued...

- ▶ Windows uses IE security zones
- ▶ Tracks origin within the NTFS alternate data stream
- ▶ Allows Windows to present suitable messages based on origin
- ▶ **Hide mechanisms to remove zone information**
  - Hides these messages
  - Makes it difficult to open downloaded files

# User Settings Still Can't be Scanned

- ▶ Stored in profiles, in NTUSR.DAT
- ▶ Dynamically loaded into HKey\_Current\_User
- ▶ Problems
  - HKCU doesn't exist if nobody is logged on
  - Scanner can't access if someone is logged on
  - User can't log on if NTUSR.DAT is loaded in scanner
- ▶ Solutions
  - Use impersonation to scan logged on user
  - Scan all profiles by creating copies of NTUSR.DAT
  - If any profile is non-compliant consider the system non-compliant




# More Settings that Won't Scan

- ▶ *Network access: Allow anonymous SID-Name translation*
  - ▶ XP, Vista, and Win
  - ▶ Stored in an unpublished manner
- ▶ *Some advanced audit policies*
  - Not supported until OVAL 5.7:

Audit Kerberos Authentication Service	Audit Kerberos Service Ticket Operations
Audit Other Account Logon Events	Audit Network Policy Server
Audit Credential Validation	Audit Detailed File Share
Audit File System	Audit Registry


# Agenda

- ▶ What Changed Since Alpha
  - ▶ What Hasn't Changed
  - ▶ How do the USGCB and FDCC Relate?
  - ▶ Building Your Test Lab
  - ▶ Resources
- 

# USGCB Versus FDCC

- ▶ The FDCC is the authoritative program
- ▶ The USGCB are the baselines for the FDCC
- ▶ Current
  - Windows 7 & Internet Explorer 8
- ▶ Near future
  - Red Hat Enterprise Linux 5 (Tier 3 DoD just posted)
- ▶ Further out
  - Apple OS X
- ▶ XP, Vista, & IE8 baselines will be reconciled with USGCB

# Agenda

- ▶ What Changed Since Alpha
  - ▶ What Hasn't Changed
  - ▶ How do the USGCB and FDCC Relate?
  - ▶ Building Your Test Lab
  - ▶ Resources
- 

# Use Our Pre-Built Lab

- ▶ VHDs have no license key.
- ▶ 30 day evaluation period, then “not genuine” pop-ups.
- ▶ **slmgr /rearm**
  - Extends the evaluation for another 30 days.
- ▶ Rearm Windows 7 or Vista three times.
- ▶ **slmgr /dlv**
  - View the amount of time remaining and rearm count.

# Build Your Own Lab

1. Install an evaluation copy of the Windows 7:
  - <http://technet.microsoft.com/en-us/evalcenter/cc442495.aspx>.
2. Install Microsoft's Security Compliance Manager (SCM):
  - <http://technet.microsoft.com/en-us/library/cc677002.aspx>.
  - You will be prompted to download and install SQL Express,
    - Need an Internet connection
    - Or you can download the SQL Express installer manually.
3. Now install the Local Policy Tool:
  1. Open the **Start** menu, click **All Programs**, click **Microsoft Security Compliance Manager**, then click **LocalGPO**.
  2. Double-click **LocalGPO.msi**.

# Build Your Own Lab Continued...

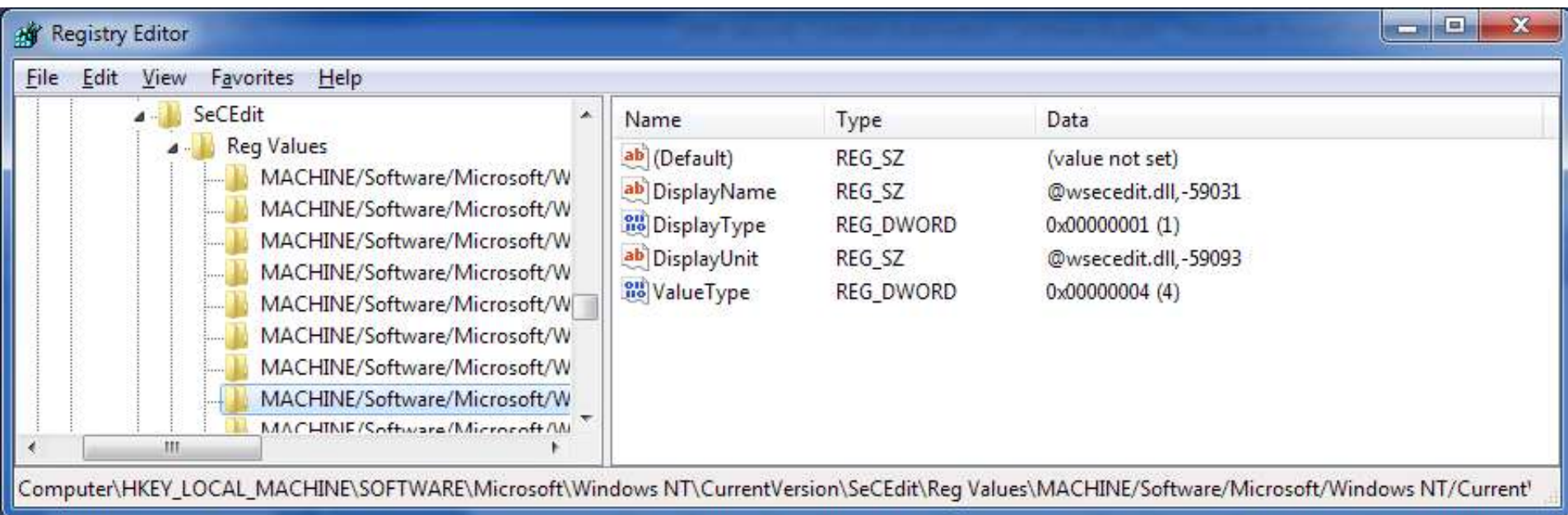
1. Right-click **LocalGPO Command Line**, and then click **Run as administrator**.
2. At the command prompt, type **cscript LocalGPO.wsf /Path:<path>** and then press **ENTER**.
3. Repeat step 2 for each GPO backups.
4. Reboot.
5. You can manually verify that settings are applied by running **gpedit.msc** with administrator privileges.

# Settings You Can't See

- ▶ FDCC includes settings prefixed with *MSS*:
  - AutoAdminLogon
  - AutoShareWks
  - NoDefaultExempt
  - Etc...
- ▶ By default they are not visible in the Security Configuration Editor
- ▶ SCEcli.dll renders the security templates UI
  - Customize *%systemroot|inf|Sceregvl.inf*
  - Reinitialize: *Regsvr32 SCEcli.dll*



# Settings You Can't See Continued...



# Local Group Policy Editor

File Action View Help




- Local Computer Policy
  - Computer Configuration
    - Software Settings
    - Windows Settings
      - Name Resolution Policy
      - Scripts (Startup/Shutdown)
      - Deployed Printers
      - Security Settings
        - Account Policies
        - Local Policies
          - Audit Policy
          - User Rights Assignments
          - Security Options**
        - Windows Firewall with Advanced Security
        - Network List Management
        - Public Key Policies
        - Software Restriction Policies

Policy	Security Setting
Microsoft network client: Digitally sign commun...	Enabled
Microsoft network client: Send unencrypted pas...	Disabled
Microsoft network server: Amount of idle time r...	15 minutes
Microsoft network server: Digitally sign commu...	Disabled
Microsoft network server: Digitally sign communications (if client agree...	
Microsoft network server: Disconnect clients wh...	Enabled
Microsoft network server: Server SPN target na...	Not Defined
MSS: (AutoAdminLogon) Enable Automatic Log...	Disabled
MSS: (AutoReboot) Allow Windows to automati...	Enabled
MSS: (AutoShareServer) Enable Administrative S...	Not Defined
MSS: (AutoShareWks) Enable Administrative Sh...	Not Defined
MSS: (DisableIPSourceRouting IPv6) IP source ro...	Not Defined
MSS: (DisableIPSourceRouting) IP source routin...	Not Defined
MSS: (DisableSavePassword) Prevent the dial-u...	Not Defined
MSS: (EnableDeadGWDetect) Allow automatic ...	Not Defined

# MSS: Settings Continued...

- ▶ Threats and Countermeasures: Security Settings in Windows Server 2003 and Windows XP:
  - <http://go.microsoft.com/fwlink/?LinkId=15159>
- ▶ Security Compliance Manager:
  - <http://technet.microsoft.com/en-us/library/cc677002.aspx>
  - Local Policy Tool
    - MSS: settings
    - Import and export local GPO
  - Windows XP, 2003, Vista, 2008, 7, IE7 & 8, Office 2007
- ▶ SCM future
  - 2008 R2, SQL 2008, Exchange 2007, Office 2010

# Agenda

- ▶ What Changed Since Alpha
  - ▶ What Hasn't Changed
  - ▶ How do the USGCB and FDCC Relate?
  - ▶ Building Your Test Lab
  - ▶ Resources
- 

# Resources

- ▶ usgcb@nist.gov
- ▶ <http://usgcb.nist.gov/usgcb.rss>
- ▶ <http://usgcb.nist.gov>
- ▶ <http://fdcc.nist.gov>
  
- ▶ <http://www.energystar.gov>
  - [http://www.energystar.gov/index.cfm?c=power\\_mgt.pr\\_power\\_mgt\\_comm\\_packages](http://www.energystar.gov/index.cfm?c=power_mgt.pr_power_mgt_comm_packages)
  - [http://www.energystar.gov/index.cfm?c=power\\_mgt.pr\\_power\\_mgt\\_win\\_task](http://www.energystar.gov/index.cfm?c=power_mgt.pr_power_mgt_win_task)